

УДК 681.3.06

Параметри криптосистеми на кривій Едвардса над розширеннями малих простих полів

Бессалов А.В., Діхтенко А.А., Яценко О.І.

Розглянуто можливість вдосконалення криптографічних систем на еліптичних кривих на базі кривих в формі Едвардса. Описаний підхід для обчислення загальносистемних параметрів криптосистеми на кривій Едвардса над розширеннями полів F_5 та F_7 . Отримано 28 наборів параметрів, що задовольняють стандартним криптографічним вимогам та можуть бути рекомендовані у майбутніх стандартах.

Рассмотрена возможность совершенствования криптосистем на эллиптических кривых на базе кривых, представленных в форме Эдвардса. Описан подход для вычисления общесистемных параметров криптосистемы на кривой Эдвардса над расширениями полей F_5 и F_7 . Получено 28 наборов параметров, которые удовлетворяют стандартным криптографическим требованиям и могут быть рекомендованы в будущих стандартах.

The refinement possibility on elliptic curve cryptosystems on the basis of the Edwards curves is considered. The approach for an evaluation of Edwards's curve domain-parametres over of F_5 and F_7 field expansions is described. 28 gangs of parametres which satisfy standard cryptographic requirements are received. They can be recommended in the future standards.

Вступ.

Криптосистеми на еліптичних кривих є основою більшості сучасних стандартів та протоколів шифрування. Паралельно із дослідженнями щодо можливих атак на еліптичні криптосистеми не менш інтенсивно відбувається процес пошуку шляхів можливого вдосконалення таких систем. Роботи [2-6] присвячені дослідженню та аналізу властивостей нормальної форми (або форми Едвардса) еліптичної кривої, які можуть бути цікаві з точки зору криптографії. Аналіз складності групової операції для кривих в формі Едвардса дозволяє стверджувати, що на сьогоднішній день вони є найбільш продуктивними, порівняно з іншими відомими формами еліптичних кривих [2, 3]. В роботі [4] розглянуто перетворення канонічної еліптичної кривої в ізоморфну криву Едвардса, наведені умови, при яких порядок кривої Едвардса має найменший кофактор 4. Оскільки криві Едвардса не стандартизовані, відкритою залишається задача пошуку

кривих, прийнятних до криптографії. В роботі [5] запропонований один із можливих шляхів розв'язання цієї задачі, а саме пошук кривих Едвардса над розширеннями полів малої характеристики, а в [6] наданий аналіз щодо складності задачі дискретного логарифмування на кривій Едвардса над розширенням малих полів.

Базуючись на результатах [2-6], в даній роботі приведений набір параметрів для реалізації криптографічної системи на кривій Едвардса над розширеннями поля малої характеристики. В результаті отримані набори з 28 примітивних поліномів та відповідних до них генераторів групи точок кривої Едвардса над полями F_5^{181} , F_5^{277} та F_7^{127} .

1. Порядки кривих Едвардса над розширеннями полів малої характеристики, прийнятні для криптографії.

Крива Едвардса над кінцевим полем F_p^m характеристики $p > 3$ в афінній системі координат визначається рівнянням [1, 2]:

$$x^2 + y^2 = 1 + d x^2 y^2, \quad \text{де } d(1-d) \neq 0, \quad d \neq A^2. \quad (1)$$

З точністю до ізоморфізму [2-4] можна вважати різними криві, що задаються різними значеннями параметру d в рівнянні (1), причому d має бути квадратичним нелишком в полі F_p^m . Будь-яка така крива має 4 обов'язкові точки:

$O = (0, 1)$ – нуль адитивної групи точок,

$D = (0, -1)$ – єдину точку другого порядку,

$\pm P = (\pm 1, 0)$ – точки четвертого порядку.

Отже, характерною властивістю кривих вигляду (1) є те, що їх порядок кратний 4. Формули додавання двох точок кривої Едвардса мають вигляд [1, 2]:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right), \quad (2)$$

Закон додавання є повним і визначений для будь-яких двох точок (x_1, y_1) , (x_2, y_2) , якщо d – квадратичний нелишок в полі F_p^m [2].

В роботі [5] детально розглянуто один із можливих способів знаходження кривих Едвардса вигляду (1), в межах прийнятних криптографічних значень параметрів. Ідея полягає у знаходженні кривої Едвардса мінімального порядку 4 над полем F_p малої характеристики та подальшому розширенні поля з метою відбору простих степенів розширення m , при яких знайдена крива над полем F_p^m має майже просте значення порядку $N_{Em} = 4n$ (де n – просте). В [5] отримано три розширених поля характеристики $p = 5$ або $p = 7$ для яких крива $x^2 + y^2 = 1 + 3x^2y^2$ має псевдопросте значення порядку, що задовольняє стандартним вимогам до порядку генератора криптосистеми. Отримані поля наведені в таблиці 1 відповідно до величини поля в бітах та значення $n = N_{Em}/4$.

Розширення полів характеристики $p = 5$ та $p = 7$ та відповідні прості порядки підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$ Таблиця 1

F_p^m	m_b	$n = N_{Em}/4$
F_5^{181}	420	4D1E1043D31FB1CC9B562A717B3C43259476330974981C14F25E03EACA14C7378C72BEB6F54DB72B8180B352DF12BA34CC023C219
F_5^{227}	527	21C529DD78FA571E196B3EBB0D20429C476A1848CAB5E0E8A121378DE187888F99D299F404EE4F9BC974D5035A62AC9F5E1E0DA29A510B4012E23ECD15909A4B1065
F_7^{127}	356	5CAC4104D859A6DF582D5731211D9947A4AE9CFD1F4E3648997D050DCE03624B891381F19AA1824CF98DE5637

Слід зауважити, що арифметичні операції в полях малої характеристики та їх розширеннях, як правило, виконуються більш ефективно порівняно з простими полями великої характеристики [5]. Крім того, криві зі малим значенням параметру $d = 3$ дають можливість зменшити складність операції додавання різних точок на $1U$ - одну

польову операцію множення на параметр кривої [2, 4], оскільки множення на 3 замінюється трикратним додаванням у полі (тобто практично безкоштовною операцією).

2. Обчислення параметрів криптосистеми на кривій Едвардса над розширеннями малих полів.

Подальша реалізація рекомендованих у [5] кривих Едвардса над розширеннями полів F_5 та F_7 представляє собою два послідовних етапи:

- пошук примітивних поліномів $P(z)$ для полів F_5^{181} , F_5^{277} , F_7^{127} та побудова відповідної арифметики цих полів;
- обчислення генератора абелевої групи точок кривої згідно з визначеною арифметикою полів F_5^{181} , F_5^{277} та F_7^{127} .

Таким чином, за допомогою прикладної програми був отриманий ряд примітивних поліномів вказаних полів, серед яких ми обрали поліноми найменшої ваги. (Слід зазначити, що для випадку поля F_7^{127} існують примітивні поліноми найменшої можливої ваги – тобто триніми). У загальному випадку точками кривої будуть пари (x, y) елементів поля F_p^m , для яких виконується рівність (1). Щоб отримати генератори підгруп точок досліджуваної кривої Едвардса $x^2 + y^2 = 1 + 3x^2y^2$, вибираємо випадкову координату x з елементів відповідного поля та обчислюємо значення $a = \frac{1-x^2}{1-3x^2}$. Визначення квадратного кореня з елементу a в розширеному полі робиться за допомогою експоненціювання [4].

У випадку полів характеристики 5: $q = 5^{181} \equiv 5 \pmod{8}$ або

$$q = 5^{277} \equiv 5 \pmod{8}.$$

В мультиплікативній групі поля F_q , якщо $a = y^2$ – квадратичний лишок, маємо елементи підгрупи F_5^* :

$$a^{\frac{q-1}{2}} = 1, \quad a^{\frac{q-1}{4}} = \pm 1 = \delta, \quad \delta^{\frac{1}{2}} = \pm 2.$$

$$\text{Тоді } a = \delta a \cdot a^{\frac{q-1}{4}} = \delta \cdot a^{\frac{q+3}{4}} \Rightarrow y = \delta^{\frac{1}{2}} \cdot a^{\frac{q+3}{8}}.$$

$$\text{Для поля характеристики 7: } q = 7^{127} \equiv 3 \pmod{4}.$$

Аналогічно, оскільки $a = y^2$ – квадратичний лишок, маємо:

$$a^{\frac{q-1}{2}} = 1, \quad a^{\frac{q-1}{2}} a = a^{\frac{q+1}{2}} = a, \quad \Rightarrow \quad y = a^{\frac{q+1}{4}}$$

Таким чином отримаємо пару (x, y) , що задовольняє рівності $x^2 + y^2 = 1 + 3x^2y^2$, значить точка $Q = (x, y)$ належить до кривої Едвардса. Помноживши Q на величину n з таблиці 1, можемо отримати точку нуль $O = (0, 1)$, точку $D = (0, -1)$ другого порядку або точки $\pm P = (\pm 1, 0)$ четвертого порядку. В першому випадку генератором G підгрупи точок кривої Едвардса буде власне точка $G = Q = (x, y)$, в інших – генератор G визначається як $G = 2Q$ або $G = 4Q$ відповідно. Результати обчислень, а саме, примітивні поліноми та генератори підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$ для відповідних полів, наведені в таблицях 2-4 (молодші степені векторів – зліва).

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{181} .

Таблиця 2

$$P(z) = z^{181} + z^3 + z^2 + 3z + 3$$

$x = [02014203431002222410101222130414030143220324303224112443420401214111010112403334214034124304424123141311100134012122333201431140043232321300324240122244440432240430443332240124213444]$

$y = [3324300121131021231010223322214342013444333012441104432413222344114310100321144203343441124124324310210144323042413441103201032141100413114111433042433133303044101341124422443002304]$

$$P(z) = z^{181} + z^3 + 4z^2 + 3z + 2$$

$x = [0032213411201001214310332324114032301222413113232102442424013032143111433023110100343142203133440433332220322232244442411423314030420411224034442134440131343004334020340401303330243]$

$y = [030430204201141033440121201004420123233110441401320234130413132430332314112324002304112100120314202043203010241004311331222434423031243233323200023131134221110113111233041334110303]$

$$P(z) = z^{181} + 2z^4 + z^3 + 2z^2 + 2$$

$x=[2200402300410434044201334124221330022144213001021002130000143$
 $4240420343313030141104330144333413340343024321400343321440234041$
 $3103210401232142442030124341024334330424232440120113002]$
 $y=[3243001344244220043044431430113232102142201102042300033033043$
 $3220042421231342032124423311220411110032130411310122130422024031$
 $02042104001441121141321103434420432223241130202133122232]$

$$P(z) = z^{181} + 3z^4 + z^3 + 3z^2 + 3$$

$x=[0114332041022410244313233331434040302303021211041400322341302$
 $1220321331241431011032002233400122124044144113420032242042334302$
 $0343343324131140104122114122431314220110124242443242042]$
 $y=[3114133140044001024344422144014114312224104023323224211041201$
 $4430324133402033304240223121331201143242330021300003321131302000$
 $2231440302241203004141444211110400022431042343111443331]$

$$P(z) = z^{181} + z^5 + z^3 + 2z + 2$$

$x=[2301312404114440140043310234301122301224212000324224433312430$
 $4321034123423142234023344404023112002114430330430032412131320102$
 $42434400113114402014243140410422030102020414113441220344]$
 $y=[0334341230414311414224334011034041233420442331334423434424432$
 $2332440313342314143401100301244143333402322114103421234414440033$
 $41210322402032100033042421030133302441101343342401104112]$

$$P(z) = z^{181} + z^5 + z^3 + 2z + 3$$

$x=[0333311434442111324403301130103313221202030422040211300031102$
 $2412232411123230414321301143243032104000340233431340412031414111$
 $0203301342312133204014433102201121414213103210020233233]$
 $y=[2244330210124231021334244202113220114201140100322232201432340$
 $0102001304032340241310401142300200043100014324134441231114132413$
 $24431001304331413224301101321240311333112331101113212222]$

$$P(z) = z^{181} + z^5 + 2z^4 + 3z^3 + 2$$

$x=[4013132032421411004141403414021320313402042110103043013044330$
 $0024130320220432233321031014300111443004243330211032340344114211$
 $10104031334201023011202223030412124230220042400140141442]$
 $y=[2330043024402424001141140431122232214314400103402101103304141$
 $1341434223343244331320024420121003143213443142041401330343204021$
 $10001024001444230030123042041244110222422144421134021042]$

$$P(z) = z^{181} + z^5 + 3z^4 + 3z^3 + 3$$

$x=[430231143030042104122442004211031442233231212331100100323003341201344433331120310002101312011223223204122134310412131024210020010344000212342212231041402210200331004344113222024213]$

$y=[220214013224431013231414442230343012344044044401130023141411412230431411443324442143420222112422320020233343333111224420014110214141313101211024203211233332014432024110101244422032]$

$$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 2$$

$x=[2133031200431014104302141130002230424014234304401044412332342040132410210214100122121311131300130103000344310140442442340320014244204102221243131002143020320441413104121022010011224]$

$y=[3333422234030121144044221420100232100211411304304423020232044314143134444103212330002031200221412223342333423040032120031121042103413314034213433320313204204142423432231111343131424]$

$$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 3$$

$x=[0410043102201244000103230003234444034321342101120410430303414124224202421024021331132111122000322143010203144300231242304004012413201210031430442213132323404140011111132002424240024]$

$y=[1033001323114344203431043410314243400431244014204032342032022442143130304400401440301120142011040403241340200311120100402011011001013222110040301404424424444430412234131012102303002]$

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{277} .

Таблиця 3

$$P(z) = z^{227} + z^3 + 2z^2 + z + 2$$

$x=[20043420420034224242113233011331103312243140433324224401023133034044014334131014234324042212220121440222212300220240300213414410003223301423214412331320424230214324143212211313402442210201011301233331023424341241030110010244112]$

$y=[14331402130021030411131044234411403113101314313344120411204430011341141020233102332044333322414233444240324231133331313330432043114002101324230113243123130004140421004224114013220133132402444210021203120142144034202041300112124]$

$$P(z) = z^{227} + z^3 + 3z^2 + z + 3$$

$x=[3202212011144112223243103140213230314040422231410023323013133$
 $0211024433203113014314130344404113033202441041221121240132322400$
 $2210342140411344214404423041332423202410344324144233101420230340$
 $10432303410314333344123110324133014444]$
 $y=[0011202100003303030404201442334410440144220432442010012323421$
 $1343220410234021302240342024043403011301404024011333412120213233$
 $0041432214331030022322230431302444340121231104230313110122024422$
 $42303132014031113111234342422020044441]$

$$P(z) = z^{227} + z^4 + 2z^2 + z + 2$$

$x=[0013034113131201242121204014024031301420234043142001004420031$
 $3404102301334141242324123210333142033414113314031314413000113222$
 $2214402120040222430131433321234031143331414443402413000302044033$
 $41112121434014142324330221001112410233]$
 $y=[0031432330103422042043320033030433242323004324041110302010103$
 $4122314222141341104433434122243404422030404334223334303034040424$
 $4010411242423444001043242321123013001422203204430401413322302220$
 $13431233200332300420214144122220040011]$

$$P(z) = z^{227} + 2z^4 + 4z^3 + 2z + 3$$

$x=[0414304013132321133130203302320444322412442302134321034100341$
 $4444033213324434332221104012340233034200120441212232122404211210$
 $0334111230131020230020231203434301432043130111332211340014304442$
 $31340213300421434310222012014001304312]$
 $y=[4223034330024341021203012302024210001130212430321044014100244$
 $3241020441144112034004242310442233112340411042343130421314112244$
 $0312211111132142124201114221440134040423413024241430141344003031$
 $40332312122230440412412014214104242112]$

$$P(z) = z^{227} + 3z^4 + 4z^3 + 2z + 2$$

$x=[4243112010013241010140212314040230001343303414112441042114223$
 $2234430434120401121023214001134341202002213410434423032400123012$
 $0134302002411031032231224424202403241420441041002400042331314204$
 $24303114010414324324130040420431221312]$
 $y=[2323210234201411223120343341311223033044310040323320402304012$
 $4003030212110124431223141434223110141130003014112014223414410344$
 $2404432201142421403112420300030200220433031032233440132302022420$
 $02334432013101442113041341131031430241]$

$$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$$

$x=[2430334213104423120424034201103222200130221242234112430021030$
 $4133423242121230234243044432440011442411134133222320440241231131$
 $3044320002023232102241443012142241224120334231443021114444001103$
 $10141404400033033330022313312132242401]$
 $y=[4010221013301134403402100242102003414142030310142133132414422$
 $1410320010321143014134030033032023410234330304043201320120331223$
 $2103030322243412213230031431102343112124441432430442033231234231$
 $142300143241243130422244022030313101]$

$$P(z) = z^{227} + z^6 + 2z^3 + 3z + 2$$

$x=[4134341234312012133334200031313033223042313140214114320001024$
 $3111304221133241011324424303433302322122122022133330013424344010$
 $0214244422311231332420421242412424432200444101312142321302243332$
 $04101014144141323112113143340440320304]$
 $y=[4234134024124442230044044024222133021200131241204111422133120$
 $4134443000440111002000141312344244104034224311222404020431110333$
 $4410120140334010311000202121302010211221224012441210143124343014$
 $30040141131032043411000444241002004334]$

$$P(z) = z^{227} + z^6 + 3z^3 + z + 3$$

$x=[1340034433202234414241033130023113401234303244004021421031433$
 $4144342412302243033102032000413012112033000441311241321003432332$
 $0231024041434233314012240000000403410341301212112102204101143024$
 $10314021421031204434324234123430414422]$
 $y=[0210334041411011441230331134121003100324330310432211130324332$
 $4030244003103023104232420221234332223111020343134121220432022130$
 $4330001212034320103201103303013312331320101203244031423413102202$
 $00300141314144212422121234042041232021]$

$$P(z) = z^{227} + 2z^6 + z^4 + 2z^2 + 2$$

$x=[3243043220444114413040121114103402110200313044400111401130430$
 $1313433441123000142403411000400241433323230400134043303013343004$
 $0302114131312314300010300223224101413402424043221131224232442220$
 $40423221042213312140403221123420220143]$
 $y=[1042043333300402021130201011311113102412123243003330424224303$
 $0003102014401040010430212034430124413432331321310232423322241243$
 $1231402201314221021124221000142030402121313000010144342242211414$
 $1123411242211320034120331300313304424]$

$$P(z) = z^{227} + 2z^6 + 3z^4 + 4z^2 + 3$$

$x=[02124203121121324411200224140411102320211132444243110341144403332421234003140123120411042423013102433344041411420133023011103223400200431141020403033114412130332424342132443301332100234223114013114320024111430010043412323030441]$

$y=[43424210212234423234101402131204120131221240003311022232424130102024343134034323320333441003124123322112414420123021202100333444011423323000043442110340122330042040310412322120443044300230112104222243003134330440302014342021402]$

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_7^{127} .

Таблиця 4

$$P(z) = z^{127} + 3z^2 + 2$$

$x=[4604400660314530520140512320422253003101622251620100566120424442252252336332411326652522200545462324056314665441612464210212622]$

$y=[1315146304405536605163143524011444005506405005503645401564462356545524016162320562506421202443621520151462064365205315315304604]$

$$P(z) = z^{127} + 5z^2 + 4$$

$x=[0365543336521056434115462035132645453515116101365233056655305116255245641440542111144453630655165504056253603613366510226532136]$

$y=[1320535462026604260101544426213561204115341115602220323203333433245626153121213266065661140060063151124413335506214231326452465]$

$$P(z) = z^{127} + 2z^2 + 2z + 4$$

$x=[6466315652246436042461332262106126432515514661254665034016552646065626060533060100124152436553211224254636165342324366353310533]$

$y=[0542300453462463464514434656410646414215130311546555534055221451454254241551363205015460054452205115415343155225440134323016614]$

$$P(z) = z^{127} + 4z^2 + 2z + 2$$

$x=[15603613433453201456440343246134161662326116262564562611065413611640150064354520322441435430203152405222336106160316230450346]$

<p>46]</p> <p>y=[2256513651540410321435461410010262042443261020443422150552652063161012010330413103413553244242502116002063560434533056053213245]</p>
<p>$P(z) = z^{127} + 2z^3 + 6z^2 + 2$</p> <p>x=[5102324002515120030151314655562511233351431342531261540462463336354446411240214323110454664456241163315166464334525262210322422]</p> <p>y=[3145460036400223043531652220003565363065332633610553433026016436223364053513240501226115355225601143615015051412330604553555305]</p>
<p>$P(z) = z^{127} + 4z^3 + 3z^2 + 4$</p> <p>x=[0321044602215515306163604444534654355456653223402115426626464300655343162133633045235434233041632113023300651041351634651260421]</p> <p>y=[6430045662343111666236354003534065352354001601500445556515134623303552646655402641601055640532033333633131360641131036456656113]</p>
<p>$P(z) = z^{127} + 3z^5 + 2z^2 + 4$</p> <p>x=[3605540632530630020020621400203533666351210044511512214312646320433252362113163133121310640460105030112645106624021354014363116]</p> <p>y=[5023342324043014040255000360213550203505533503305662126320400053300620023316045515325260316610631040513610501502366223621126616]</p>
<p>$P(z) = z^{127} + 6z^5 + 4z^2 + 2$</p> <p>x=[2635363263655442624325313520650033524341646630112166453301105654641432102355256221541423030245011614506021004161054435615630562]</p> <p>y=[4064320322316346532460245142503351460346245334541212054654612453350030043656534115440136536565561316466450122051462623003162233]</p>

Висновки.

З практичної точки зору питання щодо реальних оцінок швидкодії криптосистеми на кривій Едвардса над розширеннями малих полів

залишається відкритим. Однак теоретичні дослідження дозволяють стверджувати, що параметри, надані в таблицях 2-4, забезпечать максимальну продуктивність криптосистеми при заданій стійкості.

Отримані параметри можна розглядати як еквівалентні відносно продуктивності при однаковому рівні стійкості системи. Виключення складає випадок поля F_7^{127} : для цього поля знайдено два примітивних поліноми ваги 3, тому відповідна арифметика поля є більш прийнятною порівняно з арифметикою, що побудована відповідно до поліномів більшої ваги. Незначна втрата стійкості [6] криптосистеми на кривій Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полями F_5^{181} , F_5^{227} та F_7^{127} , складає 4 біта в кожному з трьох випадків та є незначною порівняно з величинами відповідних полів в бітах.

В цілому вважаємо, що отримані параметри можна рекомендувати при побудові продуктивних криптосистем та розробці проектів майбутніх стандартів та протоколів.

Література

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2007, PP. 1-20.
3. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. С.33-36.
4. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

5. Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей. Прикладная радиоэлектроника, 2012, Том 11, №2. С. 225-227

6. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Оценка реальной стойкости криптосистемы на кривой Едвардса на расширениях малых полей. Сучасний захист інформації, №2, 2012. С.17-20.

7. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб.пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

ПРЭ №2, 2013